

111TH CONGRESS
1ST SESSION

H. R. 2165

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity threats to the reliability of the bulk power system, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 29, 2009

Mr. BARROW (for himself, Mr. MARKEY of Massachusetts, and Mr. WAXMAN) introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity threats to the reliability of the bulk power system, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Bulk Power System
5 Protection Act of 2009”.

6 **SEC. 2. FINDINGS.**

7 The Congress finds that—

1 (1) it is in the public interest to require the
2 Federal Energy Regulatory Commission to promptly
3 order measures to address known cybersecurity
4 threats to the reliability of the electric bulk power
5 system; and

6 (2) the Commission must have the necessary
7 emergency authority to respond promptly to future
8 cybersecurity threats that could compromise reli-
9 ability of the bulk power system.

10 **SEC. 3. PROTECTION OF BULK POWER SYSTEM FROM CY-**
11 **BERSECURITY THREATS.**

12 (a) IN GENERAL.—Part II of the Federal Power Act
13 is amended by adding the following new section after sec-
14 tion 215:

15 **“SEC. 215A. EMERGENCY AUTHORITY TO ADDRESS CYBER-**
16 **SECURITY THREATS TO THE BULK POWER**
17 **SYSTEM.**

18 “(a) DEFINITIONS.—For purposes of this section:

19 “(1) The terms ‘reliability standard’, ‘bulk
20 power system’, ‘reliable operation’, ‘cybersecurity in-
21 cident’, ‘Electric Reliability Organization’, ‘regional
22 entity’, and ‘owners, users or operators’ shall have
23 the same meaning as when used in section 215.

24 “(2) The term ‘cybersecurity threat’ means that
25 there is credible information or evidence of—

1 “(A) a likelihood of a malicious act that
2 could disrupt the operation of those program-
3 mable electronic devices and communications
4 networks including hardware, software and data
5 that are essential to the reliable operation of
6 the bulk power system; and

7 “(B) a substantial possibility of disruption
8 to the operation of such devices and networks
9 in the event of such a malicious act.

10 “(3) CLASSIFIED INFORMATION.—The term
11 ‘classified information’ means any information that
12 has been determined pursuant to Executive Order
13 12958, as amended, or successor orders, or the
14 Atomic Energy Act of 1954, to require protection
15 against unauthorized disclosure and that is so des-
16 ignated.

17 “(4) SENSITIVE CYBERSECURITY INFORMA-
18 TION.—The term ‘sensitive cybersecurity informa-
19 tion’ means unclassified information that, if an un-
20 authorized disclosure is made, could be used in a
21 malicious manner to impair the reliability or oper-
22 ations of the bulk power system or the supply of
23 electricity to the bulk power system.

24 “(5) The term ‘Secretary’ means the Secretary
25 of Energy.

1 “(b) INTERIM AUTHORITY TO ADDRESS EXISTING
2 CYBERSECURITY THREATS.—

3 “(1) IN GENERAL.—After notice and oppor-
4 tunity for comment, and after consultation with ap-
5 propriate governmental authorities in Canada and
6 Mexico (subject to adequate protections against in-
7 appropriate disclosure of security-sensitive informa-
8 tion), the Commission shall establish, by rule or
9 order, within 120 days after enactment of this sec-
10 tion, such measures or actions as are necessary to
11 protect the reliability of the bulk power system
12 against the cybersecurity threats resulting from—

13 “(A) the vulnerabilities identified in the
14 June 21, 2007, communication to certain ‘Elec-
15 tricity Sector Owners and Operators’ from the
16 North American Electric Reliability Corpora-
17 tion, acting in its capacity as the Electricity
18 Sector Information Sharing and Analysis Cen-
19 ter; and

20 “(B) related remote access issues.

21 Such measures or actions may be required of any
22 owner, user, or operator of the bulk power system
23 within the United States.

24 “(2) ADDITIONAL ORDERS.—Until such time as
25 the interim reliability measures or actions ordered

1 under this subsection are replaced by cybersecurity
2 reliability standards developed, approved, and imple-
3 mented pursuant to section 215, the Commission
4 may issue additional orders to supplement the initial
5 rule or order issued under this subsection only if,
6 based on subsequent information or petition from an
7 affected entity, the Commission determines that
8 clarification or refinements to the originally ordered
9 measures or actions are necessary to ensure that the
10 threats are adequately and appropriately addressed.
11 Any such additional orders shall be preceded by no-
12 tice and opportunity for comment.

13 “(c) FUTURE EMERGENCIES INVOLVING IMMINENT
14 CYBERSECURITY THREATS.—

15 “(1) AUTHORITY TO ADDRESS IMMINENT CY-
16 BERSECURITY THREATS.—Whenever the President
17 issues and provides to the Commission (either di-
18 rectly or through the Secretary) a written directive
19 or determination that an imminent cybersecurity
20 threat to the reliability of the bulk power system ex-
21 ists, the Commission may on its own motion, with or
22 without notice, hearing, or report issue such orders
23 for emergency measures or actions as are necessary
24 in its judgment to protect the reliability of the bulk
25 power system against such threat.

1 “(2) CONSULTATION.—Before acting under this
2 subsection, to the extent feasible, taking into ac-
3 count the nature of the threat and urgency of need
4 for action, the Commission shall consult with appro-
5 priate governmental authorities in Canada and Mex-
6 ico (subject to adequate protections against inappro-
7 priate disclosure of security-sensitive information),
8 entities described in paragraph (3), and officials at
9 other Federal agencies, including the Secretary, as
10 appropriate, regarding implementation of measures
11 or actions that will effectively address the identified
12 threat.

13 “(3) APPLICATION OF EMERGENCY MEAS-
14 URES.—An order for emergency actions or measures
15 under this subsection may apply to—

16 “(A) the Electric Reliability Organization
17 referred to in section 215,

18 “(B) a regional entity with respect to the
19 United States operations of the Electric Reli-
20 ability Organization,

21 “(C) the regional entity, or

22 “(D) any owner, user, or operator of the
23 bulk power system within the United States.

24 “(d) DISCONTINUANCE OF INTERIM MEASURES.—
25 The Commission shall issue an order discontinuing any

1 measures or actions ordered under subsection (b) upon the
2 earliest of the following:

3 “(1) When the President (either directly or
4 through the Secretary of Energy) issues a written
5 order or directive provided to the Commission to the
6 effect that the threat to the bulk power system that
7 requires such measures, or actions no longer exists.

8 “(2) When the Commission determines in writ-
9 ing that the ordered measures or actions are no
10 longer needed to address the identified threat.

11 “(3) When a reliability standard developed and
12 approved pursuant to section 215 is implemented to
13 address the identified threat.

14 “(4) One year after the issuance of an order
15 under subsections (b) unless the President (either
16 directly or through the Secretary) issues a deter-
17 mination affirming the continuing nature of the
18 threat. A determination issued under this paragraph
19 shall expire upon the implementation of a standard
20 under section 215 to address the identified threat.

21 The Commission shall issue such order to be effective
22 within 30 days of the relevant triggering event set out in
23 paragraphs (1) through (4).

24 “(e) DISCONTINUANCE OF EMERGENCY MEAS-
25 URES.—The Commission shall issue an order dis-

1 continuing any measures or actions ordered under sub-
2 section (c) upon the earliest of the following:

3 “(1) When the President (either directly or
4 through the Secretary of Energy) issues a written
5 order or directive provided to the Commission to the
6 effect that the threat to the bulk power system that
7 requires such measures, or actions no longer exists.

8 “(2) When the Commission determines in writ-
9 ing that the ordered measures or actions are no
10 longer needed to address the identified threat.

11 “(3) When a reliability standard developed and
12 approved pursuant to section 215 is implemented to
13 address the identified threat.

14 “(4) With respect to orders under subsection
15 (c), one year after the issuance of an order unless
16 the President (either directly or through the Sec-
17 retary) issues a determination reaffirming the con-
18 tinuing nature of the threat. A determination issued
19 under this paragraph shall expire upon the imple-
20 mentation of a standard under section 215 to ad-
21 dress the identified threat.

22 The Commission shall issue such order to be effective
23 within 30 days of the relevant triggering event set out in
24 paragraphs (1) through (4).

1 “(f) PROTECTION OF UNCLASSIFIED SENSITIVE CY-
2 BERSECURITY INFORMATION.—

3 “(1) CONFIDENTIALITY PROCEDURES.—After
4 notice and opportunity for comment, the Commis-
5 sion shall promulgate rules and procedures to pro-
6 hibit the unauthorized disclosure of unclassified sen-
7 sitive cybersecurity information—

8 “(A) which was developed or used in con-
9 nection with the implementation of this section,

10 “(B) which specifically discusses cybersecu-
11 rity threats, vulnerabilities, mitigation plans or
12 security procedures, and

13 “(C) the unauthorized disclosure of which
14 could be used in a malicious manner to impair
15 the reliability or operations of the bulk power
16 system or the supply of electricity to the bulk
17 power system.

18 Such rules and procedures shall require the inven-
19 tory and safeguarding of such information during its
20 creation, storage and transmittal by the Commission
21 or by any other entity, including any vendor, con-
22 tractor or consultant.

23 “(2) LIMITED DISCLOSURE TO ENTITIES SUB-
24 JECT TO COMMISSION ACTION.—In the rules and
25 procedures promulgated under paragraph (1), the

1 Commission shall authorize the release of sensitive
2 cybersecurity information to entities subject to Com-
3 mission action under this section and to their em-
4 ployees, contractors and third-party representatives,
5 to the extent necessary to enable such entities to im-
6 plement Commission rules, orders or measures. En-
7 tities originating, receiving or possessing such infor-
8 mation shall comply with Commission rules and pro-
9 cedures to limit disclosure of such information to
10 any other entities that have been determined to have
11 a need to know, have executed non disclosure agree-
12 ments, and have been deemed by the entity to be
13 trustworthy and reliable. Any entity which signed
14 such non disclosure agreement and was found by the
15 Commission or by another entity subject to this sec-
16 tion to have improperly disclosed sensitive cybersecu-
17 rity information shall thereafter be denied access to
18 such information, and the Commission shall suspend
19 ability of the entity disclosing such information to
20 appear before the Commission. The sanctions under
21 this paragraph against any individual or other entity
22 shall be in addition to, and not in lieu of, any other
23 actions Commission is authorized to take pursuant
24 to section 316A for failure to comply with the rules
25 or procedures established by the Commission under

1 this section. Information designated sensitive cyber-
2 security information pursuant to this section shall
3 not be subject to disclosure under the Freedom of
4 Information Act (5 U.S.C. 552).

5 “(3) LIMITATIONS.—

6 “(A) The Commission shall consult with
7 national security or national intelligence agen-
8 cies, as appropriate, for purposes of designating
9 certain information as sensitive cybersecurity
10 information, but shall not designate as sensitive
11 cybersecurity information any information that
12 has been classified by another Federal agency.

13 “(B) Nothing in this section shall be con-
14 strued to authorize the withholding of informa-
15 tion from the committees of the Congress with
16 jurisdiction over the Commission or the Comp-
17 troller General.

18 “(C) In promulgating and implementing
19 rules and procedures under this section, the
20 Commission shall protect from disclosure only
21 the minimum amount of sensitive cybersecurity
22 information necessary to protect the reliability
23 or operations of the bulk power system or the
24 supply of electricity to the bulk power system.
25 The Commission shall segregate sensitive cyber-

1 security information within documents, elec-
2 tronic communications, and rules, orders or
3 records associated with such rules and orders,
4 wherever feasible, to facilitate disclosure of in-
5 formation which is not designated as sensitive
6 cybersecurity information.

7 “(D) Information may not be designated
8 as sensitive cybersecurity information for longer
9 than 10 years, unless specifically redesignated
10 by the Commission.

11 “(E) The Commission is authorized to re-
12 move the designation of sensitive cybersecurity
13 information, in whole or in part, from a docu-
14 ment or electronic communication if the unau-
15 thorized disclosure could not be used to impair
16 the reliability or operations of the bulk power
17 system or the supply of electricity to the bulk
18 power system.

19 “(4) CONSISTENCY OF MARKINGS.—The Com-
20 mission is authorized to place markings on docu-
21 ments, in whole or in part, which designate the de-
22 gree of sensitivity and limitations on dissemination.
23 Regulations and related procedures may be modified,
24 as appropriate, to ensure consistency with applicable

1 Executive Orders or laws pertaining to controlled
2 unclassified information.

3 “(5) NONDISCLOSURE OF SENSITIVE CYBERSE-
4 CURITY INFORMATION IN RULES OR ORDERS.—If a
5 rule or order issued pursuant to this section contains
6 sensitive cybersecurity information or if information
7 in the record associated with such rule or order con-
8 stitutes sensitive cybersecurity information, the
9 Commission may make the rule, order or informa-
10 tion non-public in whole or in part. The Commission
11 may disclose such non-public rule, order or informa-
12 tion to entities other than the recipient of the rule
13 or order, as the Commission deems necessary, to
14 carry out the rule or order and protect the reliability
15 of the bulk power system.

16 “(6) JUDICIAL REVIEW OF DESIGNATIONS.—
17 Any determination by the Commission concerning
18 the designation of sensitive cybersecurity informa-
19 tion shall be subject to judicial review pursuant to
20 subsection (a)(4)(B) of section 552 of title 5 of the
21 United States Code.

22 “(g) REVIEW.—The Commission shall act expedi-
23 tiously to resolve all applications for rehearing of orders
24 issued pursuant to this section which are filed under sec-
25 tion 313(a). Any person or other entity seeking judicial

1 review pursuant to section 313 may obtain such review
2 only in the United States Court of Appeals for the District
3 of Columbia Circuit. In the case of any petition for review
4 involving rules or orders containing or relating to security-
5 sensitive information, the Commission and parties shall
6 develop with the court appropriate measures to ensure the
7 confidentiality of such information, including, but not lim-
8 ited to, court filings under seal or otherwise in non-public
9 form, or judicial review in camera.

10 “(h) ENFORCEMENT DISCRETION.—The Commission
11 is authorized to impose penalties pursuant to section 316A
12 for any violation of a rule or order of the Commission
13 under this section. The Commission shall exercise its dis-
14 cretion in engaging in enforcement actions under this sec-
15 tion to recognize good faith efforts to comply with direc-
16 tives of the Commission.

17 “(i) PAPERWORK REDUCTION.—Chapter 35 of title
18 44, United States Code (44 U.S.C. 3501 et seq.) (com-
19 monly referred to as the ‘Paperwork Reduction Act’) shall
20 not apply to collections of information that relate to meas-
21 ures or actions described in this section.

22 “(j) PROVISION OF ASSISTANCE TO INDUSTRY IN
23 MEETING CYBERSECURITY PROTECTION NEEDS.—

24 “(1) EXPERTISE AND RESOURCES.—The Sec-
25 retary shall establish a program to develop expertise

1 and identify technical and electronic resources, in-
2 cluding hardware, software and system equipment,
3 helpful to cybersecurity protection of the electric
4 grid and all electric systems, including distribution-
5 level electric systems.

6 “(2) SHARING EXPERTISE.—The Secretary
7 shall offer to share such expertise through consulta-
8 tion and assistance with any owner, operator, or
9 user of the bulk power system, to any owner or oper-
10 ator of an electricity distribution system located in
11 the United States whether or not connected to the
12 bulk power system, and specifically to any owner or
13 operator of an electricity distribution system that
14 may provide electricity to national defense and other
15 critical-infrastructure facilities of the United States.

16 “(3) PRIORITY.—The Secretary shall consult
17 with the Commission, the Secretary of Defense, the
18 Secretary of Homeland Security, and other Federal
19 agencies to confirm the identity of States and elec-
20 tric systems serving such national defense and crit-
21 ical-infrastructure facilities, and shall assign higher
22 priority to such States and systems in offering such
23 support.

24 “(4) CLEARANCES.—The Secretary shall facili-
25 tate the acquisition by key security personnel of any

1 electric entity affected by this subsection of suffi-
2 cient security clearances to allow such personnel ac-
3 cess to information that would enable optimum un-
4 derstanding of cybersecurity threats and ability to
5 respond.

6 “(5) DEFENSE FACILITIES.—Within one year of
7 the date of enactment of this section, the States of
8 Alaska and Hawaii and the Territory of Guam shall
9 prepare, in consultation with the Secretary of En-
10 ergy, the Secretary of Defense, and the electric utili-
11 ties that serve national defense facilities in those ju-
12 risdictions, a comprehensive plan, to be implemented
13 by the relevant State and territorial governmental
14 authorities, identifying the emergency measures or
15 actions that will be taken to protect the reliability of
16 the electric power supply of the national defense fa-
17 cilities located in those jurisdictions in the event of
18 an imminent cybersecurity threat. A copy of each
19 such plan shall be provided to the Secretary of En-
20 ergy and the Secretary of Defense.”.

21 (b) CONFORMING AMENDMENT.—Section 201(b)(2)
22 of the Federal Power Act is amended by inserting “215A”
23 after “215”.

○